IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

IN RE GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION	)	C.A. No. 12-MD-2358 (SLR)
This Document Relates to: **All Actions**	)	

MEMORANDUM IN SUPPORT OF DEFENDANT POINTROLL, INC.'S MOTION TO DISMISS

Alan Charles Raul
Edward R. McNicholas
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
Telephone: (202) 736-8000
Facsimile: (202) 736-8711
araul@sidley.com
emcnicho@sidley.com

Attorneys for Defendant PointRoll, Inc.

Susan M. Coletti (#4690)
FISH & RICHARDSON P.C.
222 Delaware Avenue, 17th Floor
P.O. Box 1114
Wilmington, DE 19899-1114
Telephone: (302) 652-5070
coletti@fr.com

Attorneys for Defendant PointRoll, Inc.

DATED: January 22, 2013

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

I. Nature And Stage of The Proceedings

Plaintiffs in these twenty-four consolidated actions allege that defendants Google, Inc. ("Google"), PointRoll, Inc. ("PointRoll"), Vibrant Media, Inc., Media Innovation Group, LLC, and WPP, plc acted unlawfully by placing cookies on certain browsers. PointRoll was a named defendant in only two of the 24 consolidated actions. Plaintiffs filed their Consolidated Class Action Complaint ("Complaint" or "CAC") on December 19, 2012, naming PointRoll in only three of nine counts. MDL D.I. 46.

II. Summary Of The Argument

1. Plaintiffs claim that PointRoll, a digital advertising delivery company, violated federal anti-hacking and communications privacy statutes by placing cookies on their Safari browsers in alleged contravention of the browsers' default setting. Cookies are ubiquitous online, and no court has ever held that setting cookies – in accord with users' alleged preferences or not – violates any of the statutes invoked here – the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.*, or the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030.[1] Plaintiffs' sparse allegations provide no basis for this Court to accept theories that depart from the weight of precedent. Significantly, Plaintiffs do not and cannot allege that PointRoll violated any express undertaking or commitment in its privacy policy, as is alleged against Google. Plaintiffs' claims, if accepted, would turn most if not all third-party cookies into potential illegal "interceptions," unlawful data acquisitions or instances of criminal hacking and computer fraud. This would, of course, have broad and unpredictable impacts on the Internet and online advertising.

2. The claims against PointRoll should be dismissed under Fed. R. Civ. P. 12(b)(6)

[1] The Complaint includes claims under these federal statutes against each of the named defendants. Additional state and common law claims are brought against only Google.

because the Wiretap Act, SCA, and CFAA simply do not proscribe the use of cookies by Internet advertisers. Congress intended these statutes to prohibit and punish activities such as hacking and eavesdropping for criminal or tortious purposes. Plaintiffs' claims fail under the numerous existing precedents that have rejected claims that Internet advertising cookies – even in alleged circumvention of computer capabilities – violate these laws. Notwithstanding the Complaint's great length, the few allegations relevant to PointRoll are insufficient to state any claim for relief.

3. Plaintiffs do not plead facts suggesting that they suffered cognizable harm under the CFAA, and they must rely upon impermissible attempts to aggregate alleged losses to try to circumvent the statute's $5,000 damage requirement. Plaintiffs do not allege the facts necessary to establish any of the core elements of their Wiretap claim. Under the precise definitions of the Act, there can be no unlawful "interception" unless the "contents" of a communication were acquired. IP addresses, ID numbers, websites visited, Internet routing or transactional data, and the other technical information typically stored in cookies are simply not deemed "contents" for Wiretap purposes. Plaintiffs' SCA claim fails because they do not allege that PointRoll accessed a "facility" through which an "electronic communication service" is provided and acquired information from "electronic storage."

4. The criminal statutes at issue do not prohibit an Internet advertiser from setting cookies, and were not plausibly intended to grant Plaintiffs rights with respect to that conduct. Thus, Plaintiffs cannot rely on the alleged violation of these non-existent "statutory rights" to dispense with constitutionally required standards. Plaintiffs fail to demonstrate concrete injury-in-fact, thus they lack Article III standing, requiring dismissal of their claims.

III. Statement Of Facts / Summary Of Allegations

PointRoll designs and serves online advertisements for individual companies or ad agencies, and markets its ability to design and provide such creative, rich-media solutions. CAC

¶15, 20-21. The industry exists because commercial websites frequently make portions of their sites available for third-party advertisements served by companies such as PointRoll. CAC ¶41. When a user views a website, the browser communicates with the website's server and requests that information contained in the webpage be sent to the computer. CAC ¶128. Upon receipt of the user's request, the website server sends the site's content to the user's computer with an IP-address link to third-party advertisers' servers, such as PointRoll's, whose advertisements appear on the requested website. CAC ¶¶129-30. The user's computer obtains advertisements directly from the ad serving company's server. CAC ¶130. The Complaint alleges that Plaintiffs and other users see PointRoll ads based on an intentional interaction between the user's browser (which initiates this interaction) and PointRoll's third-party ad server, and that the PointRoll cookie is dropped on the user's computer when the ads are served. CAC ¶¶ 41, 75, 129.[2]

Plaintiffs[3] claim to use Apple computers with default Safari browser settings (CAC ¶¶10-13), and that such settings purport to block some so-called "third-party cookies" (CAC ¶73). These settings allegedly do not attempt to block cookies from "third parties" with which the user interacts directly "in some way, including" by submitting an online form. CAC ¶76. Plaintiffs allege that PointRoll cookies should have been blocked by these default settings, but were not because PointRoll employed server code as described by the Mayer article. CAC ¶¶74-75. As a result, Plaintiffs allege that PointRoll placed nine cookies on Plaintiffs' computers. CAC ¶¶130-133. Plaintiffs speculate that one of those cookies contained a unique ID created to "track

[2] If the ad serving company has already set a cookie on the user's computer, it communicates information stored in the cookie to the third-party's server. CAC ¶46. If no cookie is on the user's computer, the advertiser may create or "drop" a cookie for future visits by the user's computer. *See* Jonathan Mayer, *Safari Trackers*, WEB POLICY BLOG (Feb. 17, 2012), http://webpolicy.org/2012/02/17/safari-trackers/ (the "Mayer article").

[3] The purported class consists of all persons in the U.S. who used the Apple Safari Browser or Microsoft Internet Explorer web browsers, and visited a website from which Defendants deployed the cookies at issue in the complaint. CAC ¶191. Only allegations regarding the Safari browser users are asserted against PointRoll.

persons across the entire spectrum of websites on which PointRoll places advertisements." CAC ¶134. Plaintiffs cite and argue that a blog post of PointRoll's then-CEO Rob Gatto indicates that PointRoll intended to engage in Internet tracking. CAC ¶¶136-137. In actuality, however, the blog post relied on by Plaintiffs states that PointRoll's cookies were used merely "to determine the effectiveness of our mobile ads," and "did not involve the collection, retention or resale of any specific user information." CAC ¶136.

IV. Argument

A. Plaintiffs Fail To Plead Facts That Plausibly Support Their Claims

A court must dismiss a complaint under Rule 12(b)(6) where Plaintiffs fail to plead "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A well-pleaded claim "requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action," *Twombly*, 550 U.S. at 555. The court is not "bound to accept as true a legal conclusion couched as a factual allegation." *Iqbal*, 556 U.S. at 678-79.[4]

Plaintiffs do not plead that PointRoll is legally subject to an internal, technical "default" setting of their browser. Indeed, Plaintiffs simply assume, without any basis, that an Apple internal default setting has the force of law. But there is no allegation that PointRoll had made any commitment or other undertaking with respect to that Safari default setting, or even that the internal cookie setting was a legally binding mandate applicable to any external entity.[5]

---

[4] *See also Manuel v. Mears*, 2012 WL 4863061, at *2 n.2 (D. Del. Oct. 11, 2012) ("A claim is facially plausible when its factual content allows the court to draw a reasonable inference that the defendant is liable for the misconduct alleged.").

[5] It is telling that, despite elaborate discussion of the FTC complaint and settlement against Google in paragraphs 163 – 170 of the Complaint, Plaintiffs do not point to any binding legal standard of general applicability regarding cookies. Rather, the FTC allegations cited in the

Plaintiffs' complaint is essentially devoid of meaningful factual allegations supporting the possibility that PointRoll violated any statutes. The implausible nature of Plaintiffs' claims is exposed in paragraphs 139-145 of the Complaint,[6] which amount to nothing more than a series of negative claims about what PointRoll did *not* do or did *not* say. These core allegations fail even lenient pleading standards, let alone *Twombly* and *Iqbal*.[7] Here, Plaintiffs merely speculate and plead implausible, conclusory facts, claiming to show that PointRoll's cookies allegedly effectuated hacking, interception, and access to electronic "facilities." But Plaintiffs do not even identify what protected information PointRoll allegedly obtained from Plaintiffs; what websites they visited that displayed PointRoll advertisements; which PointRoll advertisements they viewed; or any particular content that PointRoll intercepted. In fact, the Complaint fails to plead that any specific Plaintiff received a PointRoll cookie from any specific site.

Instead, Plaintiffs speculate that PointRoll intercepted or otherwise acquired the "content" of electronic communications "derived from [their] web browsing activities." They support this by describing generic web browsing activities and by claiming, without any concrete factual allegations, that PointRoll's cookies somehow acquired the "contents" of their Internet activity. CAC ¶¶ 203, 205-206. Plaintiffs do not make factual allegations showing that the

---

Complaint turn on purported violations of a particular consent decree with one party, or specific representations regarding the Safari browser or the Network Advertising Initiative allegedly made by that party. CAC ¶167. Such allegations are not, and cannot be, asserted against PointRoll.

[6] Plaintiffs allege PointRoll "never denied [that it] never informed users or sought permission" (CAC ¶139); "never explained why [it] had not informed users or sought permission" (CAC ¶140); "never said" users consented to or authorized its alleged activities (CAC ¶141); "never explained why it did not disclose" the alleged activities until after the Mayer article and Wall Street Journal articles were published (CAC ¶142); "never pointed to any facts, or even suggested they exist" showing PointRoll "always intended to tell users" about the allege activities (CAC ¶143); "never explained how PointRoll protected, or de-anonymized, 'specific user information'" (CAC ¶144); and "never stated" that it did not collect, keep or sell aggregated user information that could be later linked to individuals (CAC ¶145).

[7] Plaintiffs must "show," not merely "allege," that they are "entitled to relief" against PointRoll. *Iqbal*, 556 U.S. at 679 (quoting Fed. R. Civ. P. 8(a)(2)).

cookies acquired any "contents" within the narrow definition of the Wiretap Act. Instead, they merely provide an *example* of how a URL supposedly *could* constitute "content" that theoretically *could* be captured by a hypothetical cookie. CAC ¶¶47, 207. The Complaint nowhere describes the "content" that any specific Plaintiff allegedly *actually* communicated anywhere online. In fact, the Gatto blog post cited by Plaintiffs states that PointRoll did not collect, retain, or resell users' specific information through the alleged use of the code and cookie technique. And Plaintiffs do not allege any facts, but only speculate, about what they think may be contained in the so-called "PRID" cookie. CAC ¶134.[8]

The Complaint fails to allege that Plaintiffs suffered any concrete harm, loss or other damage as a result of PointRoll's alleged activities. Although Plaintiffs discuss at length the theoretical value of an individual's personal information (CAC ¶¶49-67), they do not assert that PointRoll decreased the value of their information or that Plaintiffs failed to realize the putative monetary value of their personal information due to PointRoll's cookies – much less describe how placing a cookie on a computer plausibly proximately causes such harm. Plaintiffs do not allege that the presence of PointRoll cookies caused any costly impairment to their computers, or that the cookies could not be easily removed in a cost-free manner. Significantly, Plaintiffs only allege that Safari "inform[s] Safari users" that the browser will block cookies (CAC ¶71); they do *not* allege that the browser purported to impose any obligation on any advertiser or third party. Moreover, they do not allege that PointRoll violated any cookie commitment it made with

[8] *Citing* Rob Gatto, *Information Regarding Wall Street Journal Article*, PointRoll Blog, (Feb. 17, 2012), http://blog.pointroll.com/news_and_press/information-regarding-wall-street-journal-article/. The blog states PointRoll stopped setting cookies on Safari browsers. Plaintiffs imply this suggests wrongdoing, but any such inference is unwarranted. Indeed, mere publicity can affect the business choices companies make. For example, members of NAI make the business choice to undertake self-regulatory obligations going beyond what the law requires. *See, e.g.*, "Leadership, Innovation & Integrity," *available at* http://www.networkadvertising.org/ ("implementing … best practices will enhance trust and support the continued development of informative, creative, and free content and services on the Internet").

regard to the Safari browser; that PointRoll violated its own privacy policy; or that Plaintiffs even saw or relied on PointRoll's privacy policy. Instead, they attempt to rely on a number of bizarre *non*-allegations about what PointRoll did "not" say or "never" denied. CAC ¶¶139-145.

Faced with the glaring absence of factual allegations that would plausibly support Plaintiffs' claims against PointRoll, Plaintiffs rely on their attempt to connect PointRoll to the activities of Google addressed in an FTC action.[9] To contrive this connection, Plaintiffs point only to a May 2008 press release announcing that PointRoll was able to serve advertisements on Google websites. CAC ¶¶22-23. The standard advertising agreement referenced between Google and PointRoll simply provides for PointRoll to serve ads on Google affiliated websites,[10] as online ad-delivery companies like PointRoll would do for a variety of websites. Plaintiffs do not allege how the terms of that standard Internet advertising agreement relate to Safari cookies in any way, or establish any other relevant business or special arrangement between the entities.

B. Plaintiffs Do Not Establish A Cause of Action Under The CFAA

Plaintiffs' failure is made manifest when compared to actual elements of the CFAA.[11] First, Plaintiffs fail to plead sufficient facts to plausibly establish "damage or loss" as required to

[9] Plaintiffs' allegations regarding the FTC Complaint against Google have no application or relevance to PointRoll, CAC ¶¶163-70. The Complaint does not allege that PointRoll was subject to any FTC consent order, or that PointRoll had made any relevant privacy commitment or undertaking with regard to placing cookies on Safari browsers.

[10] A complete copy of the agreement, as well as subsequent amendments, is attached as Exhibits A - E. Exhibit A (Google Third Party Serving Compatibility Program Agreements, May 15, 2008). *See In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1426 (3d Cir. 1997)(documents "integral to or explicitly relied upon in the complaint" may be considered without turning a motion to dismiss into a motion for summary judgment.).

[11] The CFAA permits a civil suit by "[a]ny person who suffers damage or loss by reason of a violation of this section . . . if the conduct involves [one] of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)," 18 U.S.C. § 1030(g), which specify specific variations of damage or loss that must be suffered in order to bring a claim. *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 508 (3d Cir. 2005). Of these five factors, only one possibly relates to Plaintiffs' claims: a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I).

bring suit under the CFAA. Cookies are merely a few bytes of non-malicious code that are necessary to support intended browser functionality, and no court has found a legally cognizable injury resulting from setting Internet cookies. Indeed, "courts have consistently rejected this argument in similar contexts." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1066 (N.D. Cal. 2012)(citing cases). *See, e.g., Del Vecchio v. Amazon.com, Inc.*, 2012 WL 1997697, at *5 (W.D. Wash. June 1, 2012); *Bose v. Interclick, Inc.*, 2011 WL 4343517, at *6-7 (S.D.N.Y. Aug. 17, 2011); *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532, at *4-5 (C.D. Cal. Apr. 28, 2011); *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153, 1156 (W.D. Wash. 2001); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 503-504 (S.D.N.Y. 2001). Indeed, in *Specific Media, supra*, the court expressly rejected claims based on allegations that the cookies in question "circumvent[ed] the privacy and security controls of users who had set their browsers' to block third-party HTTP cookies" or "circumvented … the … capabilities of their computers."

The CFAA is primarily a criminal statute enacted to punish individuals who "accessed computers to steal information or to disrupt or destroy computer functionality." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130–1131 (9th Cir. 2009). The CFAA permits civil suits only in limited circumstances, 18 U.S.C. § 1030(g), such as when the actions of computer hackers result in the deletion, theft, or corruption of information; the infection of computers with viruses; or networks crashing. *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1066-69. Plaintiffs' claims regarding PointRoll's alleged use of cookies do not plausibly allege any harms to their computers. Indeed, cookies are used pervasively on the Internet to promote convenience and customization, *see Netscape Commc'ns Corp. v. ValueClick, Inc.*, 684 F. Supp. 2d 678, 682 (E.D. Va. 2009), and "[i]t is a matter of common understanding that cookies are minute in size and thus incapable of noticeably affecting the performance of modern computers." *Del Vecchio*, 2012 WL 1997697, at *5. Accepting Plaintiffs' CFAA claim, based on the theory that an internal

default setting is legally binding on third parties, would "transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012); *see also CBS Corp. v. FCC*, 663 F.3d 122, 174 n.19 (3d Cir. 2011). Courts traditionally apply the rule of lenity to avoid just such novel and unwarranted expansions of potential criminal liability.

1. **Plaintiffs Do Not Sufficiently Plead Losses Entitling Relief**

Plaintiffs' pleadings do not support the plausible conclusion that PointRoll intentionally accessed, without authorization or in excess thereof,[12] Plaintiffs' computers *and* that this action resulted in "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(a)(2)(c), 1030(a)(5)(A) & (C). *See Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio*, 2010 WL 4224473, at *3 (E.D. Pa. Oct. 22, 2010); *Consulting Prof Res., Inc. v. Concise Techs. LLC*, 2010 WL 1337723, at *6-7 (W.D. Pa. Mar. 9, 2010).

Nowhere does the Complaint plead facts suggesting how these cookies caused any "damage" or "loss" to computers or systems.[13] 18 U.S.C. § 1030(g). "Damage" requires "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). "Loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* at (e)(11). "Damage" or "loss" involves the impairment, damage, or other interference with computing systems, the data and software used by them, or the services provided by those systems. *See*

[12] Plaintiffs cite the Mayer article to allege that the defendants relied on an "exception" in the Safari code. CAC ¶¶ 75-76. Plaintiffs thus concede that PointRoll did not alter or damage their computers, but rather, interacted with an "exception" already incorporated their browsers.
[13] Because Plaintiffs fail to allege any cognizable loss or damage, there is necessarily no causation here.

CollegeSource Inc. v. AcademyOne, Inc., 2012 WL 5269213, at *15-16 (E.D. Pa. Oct. 25, 2012).

Plaintiffs do not allege that PointRoll impaired Plaintiffs' use of, or access to, their data, programs, or information; that Plaintiffs incurred any costs associated with responding to PointRoll's purported cookies, or restoring any data, program, system, or information; or that Plaintiffs lost revenue, incurred costs, or otherwise suffered any damages as a result of any interruption of service. Any argument that the installation of cookies damaged or impeded Plaintiffs' computers would be unavailing as a basis for damages or loss under the CFAA. *See, e.g., In re iPhone Application Litig.*, 844 F. Supp. 2d at 1066. Importantly, Plaintiffs do not even allege that cookies are per se damaging; or that there are no other similar cookies installed on their computers – because there are likely a large number of similar cookies on their computers. Cookies simply do not cause damage or loss as defined in the CFAA. *See Specific Media*, 2011 WL 1661532, at *4-5 (denying injury from installation of cookies that "circumvent" the privacy controls of users that had set their browsers to block third-party HTTP cookies).

Plaintiffs conclusory allegations that PointRoll "caused a loss to Plaintiffs and Class Members during a one year period aggregating at least $5,000 in value," CAC ¶¶ 225, 226, amounts to nothing more than a mere recital of the elements of the cause of action. This is plainly insufficient to support a cognizable claim. *See Iqbal*, 556 U.S. at 679. Plaintiffs' do suggest some "loss" regarding the value of Plaintiffs' personal information, CAC ¶¶ 49-67, but they omit any showing of how PointRoll impaired the alleged value of their personal information (or that it was even collected). Facing similarly gossamer allegations, numerous courts have held that alleged injuries predicated on the notional financial value of personal information have no bearing on "damage or loss" under 18 U.S.C. § 1030(e)(11).[14] Courts have thus routinely

[14] Courts in the Third Circuit consistently deny CFAA claims predicated on these sorts of "losses," such as claimed damages to business or business opportunities unrelated to damaged or

dismissed complaints claiming "loss" from allegedly unauthorized access to or use of personal information. *Del Vecchio*, 2012 WL 1997697, at *3-4; *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1068 ("[C]ourts have tended to reject the contention that [losses relating to] personal information . . . constitutes economic damages under the CFAA."); *In re Zynga Privacy Litig.*, 2011 WL 7479170, at *1 (N.D. Cal. June 15, 2011); *In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d at 525; *Bose*, 2011 WL 4343517, at *6-7.

Even if Plaintiffs had sufficiently pleaded that they suffered *de miminis* individual losses, they would not be entitled to aggregate their purported injuries to satisfy CFAA's $5,000 loss requirement. Plaintiffs do not plead facts to suggest that their purported injuries are uniform and subject to aggregation. *Id.*; *In re DoubleClick, Inc.*, 154 F. Supp. 2d at 523. And, as in the *Specific Media* cookie case, "Plaintiffs at the very least have failed to plausibly allege that they and the putative class - even in the aggregate - have suffered $5,000 in economic damages in a one year period as a result of Specific Media's actions." 2011 WL 1661532, at *6.

C. **Plaintiffs Fail To Establish A Cognizable Claim Under The Wiretap Act**

The Wiretap Act, like the CFAA and the SCA, is primarily a criminal statute which prohibits the intentional interception, or attempted interception, of the content of any wire, oral, or electronic communication. 18 U.S.C. § 2511(1)(a). Under the Wiretap Act, "interception" turns on the acquisition of "*the contents* of any…communication through use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4)(emphasis added). Accordingly, the Act does not prohibit acquisition of the non-content portions of communications. Likewise, there can be no "interception" under the Act if the alleged acquisition of data that does not involve the use of

---

impaired computers or systems. *See, e.g., Synthes, Inc. v. Emerge Medical, Inc.*, 2012 WL 4205476, at *19 (E.D. Pa. Sept. 19, 2012); *Eagle v. Morgan*, 2011 WL 6739448, at *8-9 (E.D. Pa. Dec. 22, 2011); *Consulting Prof Res., Inc.*, 2010 WL 1337723, at *8; *Crown Coal & Coke Co. v. Compass Point Res., LLC*, 2009 WL 1806659, at *8 (W.D. Pa. June 23, 2009).

a statutorily defined "device."

1. **PointRoll Did Not "Intercept" "Contents" Of Communications**

While Plaintiffs assert the legal conclusion that PointRoll "intercepted" Plaintiffs' communications with websites (*see, e.g.*, CAC ¶208), they fail to plead facts establishing that any statutory "interception" took place. To establish that an unlawful "interception" occurred, Plaintiffs must allege that PointRoll acquired the "contents" of a communication. 18 U.S.C. §2510(4). They have not done so. The Complaint does not allege facts that plausibly, or even possibly, support the conclusion that PointRoll intercepted the "contents" of Plaintiffs' communications. "Contents" under the Wiretap Act are narrowly defined – as appropriate in a criminal statute – as "information concerning the substance, purport or meaning of a communication." 18 U.S.C. § 2510(8). Indeed, Congress amended the definition in 1986 to "distinguish[] between the substance, purport or meaning of the communication and the existence of the communication or transactional records about it." S. Rep. No. 99-541, at 13 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3567. Technical Internet data like transactional information, such as user IDs, URLs, IP addresses, and other basic identifiers do not constitute "contents" under the statute. *See, e.g., In re Application of the U.S.*, 416 F. Supp. 2d 13, 18 n.7 (D.D.C. 2006) (originating IP address, originating and return header information, inbound and outbound packet payload, and the date and time of communications are not contents); *In re iPhone App. Litig.*, 844 F. Supp. 2d at 1061 ("information about the identities of parties to a communication … is not 'content'"). Indeed, Internet tracking does not violate current federal law because "[n]o expectation of privacy exists for…online transactional information, such as a user's Internet search history" including "ISP records of customers' visited websites." *United States. v. Polizzi*, 549 F. Supp. 2d 308, 393 (E.D.N.Y. 2008) (citation omitted), *vacated on other grounds*, 564 F.3d 142 (2d Cir. 2009).

Plaintiffs' vague reference to generic Internet browsing activities does not plausibly lead to the inference that PointRoll cookies intercepted any "content" whatsoever.[15] CAC ¶¶205-206. The assertion that PointRoll intercepted content-containing URLs must be disregarded here as pure speculation, as it is unsupported by a single specific example of any actual acquisition, and thus need not be accepted as true by this Court. CAC ¶205. Moreover, the absence of "contents" aside, the Complaint does not support a plausible inference that PointRoll intercepted a single communication of any of the named Plaintiffs. Plaintiffs only vaguely allege that PointRoll intercepted their "web browsing activities," CAC ¶203, but fail entirely to identify a single PointRoll advertisement or website hosting such an advertisement that Plaintiffs visited.[16] *See, e.g., Smith v. Trusted Universal Standards in Elec. Transactions, Inc.*, 2010 WL 1799456, *11 (D.N.J. May 4, 2010) (dismissing wiretap claims in the absence of "any factual averments that any of his communications were in fact intercepted").

Finally, even assuming *arguendo* that PointRoll intercepted Plaintiffs' content, Plaintiffs' claim would still fail because PointRoll was authorized by the websites on which its advertisements appeared to obtain the information users communicated to the website. As Plaintiffs concede, PointRoll was technically a party to and the intended recipient of the communication because this information was also communicated directly to PointRoll to serve the ads requested by the user's browser. 18 U.S.C. §2511(1)(a).[17] *See also In re DoubleClick,*

[15] Plaintiffs do not allege that PointRoll actually acquired any information submitted by Plaintiffs through online forms or search terms – only that the third-party web tracking could have "permitted" Defendants to record such information. CAC ¶206. Tellingly, Plaintiffs do not even cite the Mayer article, which provides the foundation for Plaintiffs' Complaint, CAC ¶¶75, 138, to suggest that the cookies in question could be used to commit unlawful wiretaps.

[16] Plaintiffs do not allege that PointRoll obtained any information regarding activities beyond those relating to user interactions with websites on which PointRoll ads were served. CAC ¶ 134.

[17] *See Smith*, 2011 WL 900096 at *10. Even if Plaintiffs did visit websites with PointRoll advertisements, the Complaint explains that PointRoll did not "intercept" electronic communications as a result. Plaintiffs explain that when a user visits a website with a PointRoll

Inc., 154 F. Supp. 2d at 510-51 (finding it implausible that a website would not be found to have authorized an ad server's access to users' communications with the website where doing so was required for the provision of advertisement content).[18] Moreover, Plaintiffs fail to plead any factual allegations that would plausibly support an inference that PointRoll engaged in the activities with the purpose of committing a tort or a crime (as opposed to normal Internet cookie activity).[19] *Cf. Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 804 (8th Cir. 2010) (using cookies is not itself intentionally wrongful conduct). Indeed, if the Court were to conclude that PointRoll's cookies were "wiretaps" giving rise to possible "interceptions," then almost all other third-party cookies could also be "wiretaps" -- broadly and unpredictably impacting the Internet.

---

advertisement, the user's computer sends a direct request to PointRoll's server for the advertisement's content. CAC ¶41. Thus, the user is communicating information directly to PointRoll. Even if the user's communication with PointRoll's server ("calling" for the ad to be delivered) contained "content"– which it does not – PointRoll cannot intercept a communication to which it is a party. *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, 2007 WL 4394447, *5 (E.D. Pa. Dec. 13, 2007).

[18] Plaintiffs cannot survive a motion to dismiss based on the naked allegation, made upon information and belief, that first party websites did not consent to PointRoll's advertising activities and use of cookies (CAC ¶210) where such assertion is inconsistent with the rest of the Complaint and is properly disregarded. *See Hirsch v. Arthur Anderson & Co.*, 72 F.3d 1085 (2d Cir. 1995) ("General, conclusory allegations need not be credited . . . when they are belied by more specific allegations of the complaint."). Consent here is clear as a matter of law.

[19] *Berk v. JPMorgan Chase Bank, N.A.*, 2011 WL 6210674, *3 (E.D. Pa. Dec. 13, 2011)(the alleged interceptor must have intended to commit a crime or tort independent of the act of recording / intercepting itself); *see also Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010) ("[T]o survive a motion to dismiss, a plaintiff must plead sufficient facts to support an inference that the offender intercepted the communication for the purpose of a tortious or criminal act that is independent of the intentional act of recording."). Even if PointRoll's cookies were assumed, *arguendo*, for present purposes to be "tracking" rather than ad "effectiveness" cookies, they are not alleged to be different in kind or degree from the myriad of such cookies on the Internet today – many of which are no doubt on Plaintiffs' own computers. For example, conventional uses of advertising metric cookies are a routine part of internet operations, such as by capping the frequency with which users see the same ad; "sequencing" the order in which ads appear to users; and measuring if and when a user sees and ad before visiting the advertiser's website. *See, e.g.*, FTC, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," p. 39 (March 2012) ("[D]rawing upon the recommendations of several commenters, the Commission agrees that…internal operations would encompass frequency capping and similar advertising inventory metrics").

2. PointRoll's Server Code Does Not Constitute A "Device"

Interception under the Wiretap Act also requires the use of a "device," defined as "any device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5). Plaintiffs postulate a novel legal theory that PointRoll's alleged server code constitutes a "device." CAC ¶201. Neither the statutory text nor the case law, however, treats such server code as a "device" under the Act. The classic "device" is an alligator clip attached to a phone line. Plaintiffs allege only that the code allowed PointRoll to place cookie text files on users' computers. CAC ¶¶130-133. PointRoll allegedly used those cookies, once set, and other unspecified "tracking systems" to "intercept" communications. CAC ¶201. Plaintiffs thus concede that the code itself was not, nor could have been, used to intercept any communications, and thereby fail to establish that PointRoll used a "device" as required by the statute. CAC ¶201.

3. Plaintiffs Do Not Establish That PointRoll Used Or Disclosed The Content Of Plaintiffs' Communications

Plaintiffs likewise do not state a claim under 18 U.S.C. § 2511(1)(a) because, in the absence of an "interception," any use or disclosure of alleged content acquired by PointRoll does not violate the Act. *Walsh v. Krantz*, 386 Fed. Appx. 334 (3d Cir. 2010) (no illegal disclosure or use without an "interception.").[20]

D. Plaintiffs Fail To State A Claim Under The Stored Communications Act

Plaintiffs' allegations are even more of a stretch under the Stored Communications Act, which is not a "catch-all statute designed to protect the privacy of stored Internet communications." *Low v. LinkedIn Corp.*, 2012 WL 2873847, at *6 (N.D. Cal. July 12, 2012).

[20] Even if an "interception" is assumed, Plaintiffs fail to allege facts sufficient to support the claim because the complaint does not contain any allegations identify any third parties to whom such information was disclosed, or that PointRoll used the content of communications. Plaintiffs try to get around their pleading obligation by claiming that PointRoll "never stated that PointRoll did not collect, keep or sell aggregated user information that can be later linked to individual users." CAC ¶145. Such a thin allegation cannot suffice after *Iqbal* and *Twombly*.

Rather, the statute prohibits specific conduct which the Complaint's factual allegations do not describe: (a) access to a "facility" through which electronic communications service is provided to obtain access to electronic communications (b) which are in "electronic storage" in such a system. 18 U.S.C. § 2701(a).[21]

1. **PointRoll Did Not Access A "Facility" Providing ECS**

Plaintiffs allege that PointRoll cookies were accessed from "browser-managed files" located on user's personal computers which had installed and utilized the Safari browser software.[22] CAC ¶217. Such "browser-managed files" on a user's computer, however, do not constitute facilities under the SCA as asserted by Plaintiffs' unsupported recitation of the statute. CAC ¶¶216-217. As other courts have made clear, mobile computers or products using the Apple operating system such as the iPhone or iPad have been held not to be "facilities" under the SCA. *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1057-58 (personal computers are not "facilities" because an individual's personal computer does not "provide an electronic communication service" simply by virtue of enabling use of electronic communication services).[23] If the computers that utilize and interact with the Internet through embedded browsers are not facilities, then *a fortiori* the embedded browser is also not a "facility."

Further, Plaintiffs do not plausibly plead that by accessing files on a user's computer – whether managed by the browser or otherwise – PointRoll accessed a facility through which an

[21] Plaintiffs do not allege that PointRoll violated 18 U.S.C. § 2701(b).

[22] Plaintiffs correctly do not assert that PointRoll's cookies constitute facilities. PointRoll is not an electronic communications service provider; it is an ad serving company that designs and provides online advertisements. CAC ¶¶ 20-21. PointRoll communicates with customers and sell its products and services through the internet, but it is well settled that such activities do not transform a company into an electronic communications service provider under ECPA.

[23] *See also Garcia v. City of Laredo*, 2012 WL 6176479, *3 (5th Cir. Dec. 12, 2012) (facilities protected by the SCA are not computers that enable the use of an ECS); *Freedom Banc Mortgage Servs., Inc. v. O'Harra*, 2012 WL 3862209, *9 (S.D. Ohio Sept. 5, 2012) (computers that enable the use of an ECS are not "facilities" under the SCA; instead, the facilities must be operated by an ECS provider and must be used to store and maintain data in electronic storage.).

electronic communications service is provided. An electronic communications service ("ECS") is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). An ECS provider supplies "the underlying service which transports the data, . . [and is] not the provider of a product or service which facilitate the data transport." *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 524 (N.D. Ill. 2011).

Plaintiffs do not allege (because they cannot) that the Safari browser acts as an Internet Service Provider ("ISP"), and not a single case has held that a browser constitutes an ECS. A browser without an ISP communicates with nobody. It is software installed on an individual's computer to view and access materials by interpreting available code to render it visually for a user interface. *See e.g.*, *FTC v. Zuccarini*, 2002 WL 1378421, *3 (E.D. Pa Apr. 9, 2002). Browsers do not provide any communications infrastructure for a computing service, as opposed to the communication lines that are required to link servers to the internet. *Id*. At most, a browser facilitates the use of ECS provided by other entities. In fact, courts have rejected the notion that maintaining a website or merely utilizing Internet access constitutes providing an ECS. *See Dyer v. Nw. Airlines Corps*., 334 F. Supp. 2d 1196, 1999 (D.N.D. 2004) (airline selling travel services over the Internet is not a provider of ECS); *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001) (Amazon.com is not a provider of ECS); *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 307 (E.D.N.Y. 2005) (a website is not an ECS).

2. **Plaintiffs' Information Was Not In "Electronic Storage" Of An ECS**

Further, Plaintiffs fail to plead that PointRoll acquired users' information from "electronic storage"[24] of an ECS. Plaintiffs claim that PointRoll violated the SCA by accessing

[24] Electronic storage constitutes "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

cookies in "browser-managed files" stored on Plaintiffs' computers and acquiring "recently updated cookies and related just-transmitted electronic communications out of random access memory." CAC ¶ 218. Case law clearly establishes that information contained in cookies stored on user computers--which also do not qualify as a "facility"--is not in "electronic storage." *In re DoubleClick, Inc.*, 154 F. Supp. 2d at 512; *see also In re Toys R Us, Inc., Privacy Litig.*, 2001 WL 34517252, *3-4 (N.D. Cal. Oct. 9, 2001). In fact, any communication downloaded to and stored on a user's personal computers falls outside of "electronic storage" once it is downloaded. *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1057-58; *Thompson v. Ross*, 2010 WL 3896533, *5 (W.D. Pa. Sept. 30. 2010); *Garcia*, 2012 WL 6176479 at *3.

Moreover, to violate 18 U.S.C. §2701(a) it is not enough that electronic communications data has been accessed in any format on any computer: "the data must have been accessed or obtained while it was within the electronic storage of the electronic communications service itself." *Thompson*, 2010 WL 3896533, at *3. As explained above, neither PointRoll nor the Safari browser is an ECS provider, thereby excluding both PointRoll's cookies and the alleged browser-managed files from the scope of the SCA.

E. Plaintiffs Fail To Establish Article III Standing Against PointRoll

Plaintiffs fail to plead any facts establishing they suffered any injury-in-fact as a result of PointRoll's alleged activities sufficient to satisfy the "irreducible constitutional minimum of standing" required under Article III. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992); s*ee also In re Google, Inc. Privacy Policy Litig.*, 2012 WL 6738343, at *5-6 (N.D. Cal. Dec. 28, 2012) (no injury in fact based upon alleged violations of a statutory right where plaintiffs fail to plead facts supporting a plausible statutory claim). Article III standing must be established, even where a statutory violation has created a cause of action, by sufficiently pleading the well known elements of (1) injury in fact, (2) causation, and (3) redressability. *Steel Co. v. Citizens for a*

Better Env't, 523 U.S. 83, 103-04 (1998); *Trump Hotels & Casino Resorts v. Mirage Resorts*, 140 F.3d 478, 484-85 (3d Cir. 1998). In light of Plaintiffs' failure to establish Article III standing, their claims against PointRoll are appropriately dismissed under Fed. R. Civ. P. 12(b)(1). *See Soc'y Hill Towers Owners' Ass'n v. Rendell,* 210 F.3d 168, 175 (3d Cir. 2000).

While the Third Circuit's opinion in *Alston v. Countrywide Fin. Corp.*, 585 F.3d 753, 763 (3d Cir. 2009) held that the invasion of rights created under the Real Estate Settlement Procedures Act of 1974 ("RESPA") constitutes injury sufficient for standing, that outcome should not control the statutes at issue here.[25] The Article III injury-in-fact standing requirement is not excused because Congress creates a new cause of action or legal rights.[26] The Supreme Court has repeatedly explained that (i) the "requirement of injury in fact is a hard floor of Article III jurisdiction that cannot be removed by statute," *Summers v. Earth Island Inst.*, 555 U.S. 488, 497 (2009), and (ii) that "Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing." *Raines v. Byrd*, 521 U.S. 811, 820 n.3 (1997).

Injury-in-fact sufficient for standing requires harm that is "concrete" and "actual or imminent," rather than conjectural or hypothetical.[27] *Vt. Agency of Natural Res. v. U.S. ex rel. Stevens*, 529 U.S. 765, 771 (2000). The statutes invoked by Plaintiffs, however, do not expressly grant rights against or with respect to Internet cookies, and have not previously been construed to

---

[25] Notably, the *Alston* defendants "barely touched on a stand-alone Article III standing argument" in their briefs. *Alston*, 585 F.3d at 762.

[26] Even if this were the case, Plaintiffs' cause of action under the CFAA, 18 U.S.C. § 1030(a), requires them to plead injury-in-fact in order to establish statutory standing.

[27] Plaintiffs baldly allege violations of statutory rights without proffering factual predicates for their claims; there is scant reason to believe Plaintiffs suffered either injury-in-fact *or* an invasion of those rights. The proper standing question is not whether PointRoll violated a statutory right, but whether the accused actions caused a redressable injury-in-fact to Plaintiffs. *See Joint Stock Soc'y v. UDV N. Am., Inc.*, 266 F.3d 164, 176 (3d Cir. 2001); *Doe v. Nat'l Bd. of Med. Exam'rs,* 199 F.3d 146, 153 (3d Cir. 1999).

protect Internet users from desired or undesired cookies. Accordingly, *Alston* does not control here because Plaintiffs simply do not allege the type of plausible statutory claims necessary to plead constitutionally sufficient injury. *See generally In re Google, Inc. Privacy Policy Litig.*, 2012 WL 6738343, at *5-6. While Plaintiffs conclude that their personal information has value, CAC ¶¶ 49-67, they fail to explain in any manner how they were harmed, injured, or damaged by PointRoll's alleged access to that data. Plaintiffs thus fail to carry their burden of alleging sufficient injury-in-fact to establish the Court's jurisdiction under Article III. *See, e.g., Specific Media*, 2011 WL 1661532 at *4-5 (declining to find economic value in personal data accessed through cookies); *In re JetBlue Airways*, 379 F. Supp. 2d at 327 ("[T]here is [ ] no support for the proposition that an individual passenger's personal information has or had any compensable value in the economy at large."); *Dwyer v. Am. Express Co.*, 273 Ill. App. 3d 743, 749 (Ill. App. Ct. 1995) (suggesting that any value is created by defendants who "categoriz[e] and aggregat[e]" personal information). Plaintiffs' reliance on implausible and incongruous statutory rights, along with ambiguous, generalized allegations of hypothetical harm to personal data, are insufficient to support Article III standing. *See Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011); *Allison v. Aetna, Inc.*, 2010 WL 3719243 (E.D. Pa. Mar. 9, 2010).

V. Conclusion

For the reasons set forth above, PointRoll respectfully request that: Plaintiffs' claims against PointRoll under the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*, the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, be dismissed under Fed. R. Civ. P. 12(b)(1), or dismissed with prejudice under Fed. R. Civ. P 12(b)(6).

Respectfully submitted,

Dated: January 22, 2013

By: /s/ *Susan M. Coletti*

Alan Charles Raul
Edward R. McNicholas
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
Telephone: (202) 736-8000
Facsimile: (202) 736-8711
araul@sidley.com
emcnicho@sidley.com

Attorneys for Defendant PointRoll, Inc.

Susan M. Coletti (#4690)
FISH & RICHARDSON P.C.
222 Delaware Avenue, 17th Floor
P.O. Box 1114
Wilmington, DE 19899-1114
Telephone: (302) 652-5070
coletti@fr.com

Attorneys for Defendant PointRoll, Inc.